


WHAT IS CLAIMED IS:

 1. An electronic voting method in which voters obtain authorization to vote from an administrator and send their vote data to a counter apparatus, and said counter apparatus performs vote counting, said method comprising the steps wherein:

(a) each of said voters encrypts the vote content corresponding to his chosen candidate by an encryptor with a public key of said counter apparatus, and

randomizes information containing said encrypted vote content by a random number to create a preprocessed text, and sends it to an administrator apparatus;

(b) said administrator apparatus verifies the validity of each voter apparatus, and

inputs said received preprocessed text into a signature generator to generate a blind signature for said preprocessed text, and sends it back to said each voter apparatus;

(c) said each voter excludes the influence of said random number from said blind signature for said received preprocessed text, and

obtains a signature of said administrator for said information containing said encrypted vote content, and sends said administrator signature and said information containing said encrypted vote content, as vote data, to said counter apparatus; and

(d) said counter decrypts said information containing said encrypted vote content, by a decryptor with a secret key corresponding to said public key, to obtain said vote content, and counts the number of votes polled for the candidate corresponding to said vote content.

2. The electronic voting method of claim 1, which comprises the additional steps: (d-0) wherein said counter inputs said encrypted vote content and said administrator signature into a signature verification part to make sure that said preprocessed text is signed by said administrator, and publishes a list of vote data containing encrypted vote contents; and (d-1) wherein said each voter makes sure that his encrypted vote content is placed on said list.

3. The electronic voting method of claim 1 or 2, wherein: said information randomizing step (a) comprises the additional steps wherein said each voter generates a tag that only he knows, and step wherein said each voter concatenates said encrypted vote content with said tag and randomizes it with said random number; and said step (d-1) comprises the additional step wherein said each voter separates said tag from said vote data on said list and makes a check to see if said tag is his.

4. The electronic voting method of claim 1 or 2, wherein: said step (b) comprises the additional step wherein said administrator publishes, as a list of voters, a list of information representing voters given said blind signature; and said step (c) comprises the additional step wherein said each voter makes a check to see if information representing him is contained in said list of voters.

5. The electronic voting method of claim 1 or 2, wherein said step (d) comprises the additional step wherein said counter publishes the result of counting of said vote content.

a3
6. The electronic voting method of claim 1 or 2, wherein: in said step (a) said each voter sends said preprocessed text to said administrator apparatus together with voter identification information; in said step (b) said administrator verifies the validity of said each voter on the basis of said voter identification information; and in said step (c) said each voter sends said vote data anonymously to said counter apparatus.

7. The electronic voting method of claim 1 or 2, wherein: said step (a) comprises the additional step wherein said each voter generates his signature for said vote content, and sends said his signature to said administrator apparatus together with said vote content; and said step (b) comprises the additional step wherein said administrator apparatus verifies the validity of said voter signature for said vote content.

8. The electronic voting method of claim 1, wherein: said counter apparatus has a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; in said step (c) said each voter sends said vote data to that one of said plurality of distributed counter apparatuses which is connected to one end of said series connection; and said step (d) comprises the additional step wherein said plurality of counter apparatuses sequentially decrypt information containing said encrypted content in their decryption parts with said partial secret keys, and said vote content is obtained

by the decryption processing in said distributed counter apparatus at the last stage of said series connection.

9. The electronic voting method of claim 1, wherein: said counter apparatus has a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; in said step (c) said each voter sends said vote data to all of said plurality of distributed counter apparatuses; and said step (d) comprises the additional step wherein said plurality of counter apparatuses individually decrypt said encrypted content in their decryption parts with said partial secret keys to generate decrypted intermediate data, and said decrypted intermediate data is sent from said distributed counter apparatuses to a predetermined one of them and decrypted into said vote content.

10. The electronic voting method of claim 8 or 9, wherein said decryption processing is a thresholding decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.

11. An electronic voting system which comprises a plurality of voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a nonanonymous communication channel, and a counter apparatus connected to each of said voter apparatuses through an anonymous communication channel, wherein:
said each voter apparatus comprises:
an encryptor for encrypting a vote content of a voter of said each

AB voter apparatus with a public key of said counter apparatus to generate an encrypted vote content;

a random generator for generating a random number;

a randomizer for randomizing said encrypted vote content with said random number to create a preprocessed text;

means for sending said preprocessed text to said administrator apparatus;

a derandomizer for excluding the influence of said random number from a blind signature of said administrator apparatus, received therefrom, for said preprocessed text to obtain an administrator signature of said administrator apparatus for information containing said encrypted vote content; and

means for sending said administrator signature and said information containing said encrypted vote content, as vote data, to said counter apparatus;

said administrator apparatus comprises:

a blind signature generator for generating said blind signature for said preprocessed text; and

means for sending said blind signature to said each voter apparatus; and

said counter apparatus comprises:

a decryptor for decrypting said information containing said encrypted vote content in said vote data with a secret key corresponding to said public key to obtain said vote content; and

a counter for performing vote counting for each candidate on the basis of said decrypted vote content.

12. The electronic voting system of claim 11, wherein: said each

AB
voter apparatus further comprises an administrator signature verification part for verifying the validity of said administrator signature for said information containing said encrypted vote content, and sends said vote data to said counter apparatus when said administrator signature is found valid; and said counter apparatus further comprises an administrator signature verification part into which said information containing said encrypted vote content in said vote data received from said each voter apparatus and said administrator signature are input for verifying the validity of said administrator signature.

13. The electronic voting system of claim 11, wherein: said each voter apparatus further comprises a voter signature generator for generating a voter signature for said preprocessed text and for sending it to said administrator apparatus; and said administrator apparatus further comprises a voter signature verification part for verifying the validity of said preprocessed text received from said each voter apparatus and said voter signature therefor, and generates said blind signature by said blind signature generator when said preprocessed text and said voter signature are found valid.

14. The electronic voting system of claim 11, wherein: said counter apparatus further comprises a vote list generator which, if said administrator signature is found valid, generates, as a vote list, a list of said vote data received from said each voter apparatus, and publishes said vote list to said voter in a manner to be accessible from said each voter apparatus; and said each voter apparatus further comprises a vote list checker for making a check to see if said

encrypted vote content of said each voter apparatus is contained in said vote list received from said counter apparatus.

15. The electronic voting system of claim 14, wherein said each voter apparatus further comprises: a tag generator for generating a tag that only said voter knows; a concatenator for concatenating said encrypted vote content with said tag to generate information containing said encrypted vote content; and a list checking part for extracting said tag from each vote data in said vote list and for making a check to see if vote data of said voter is contained in said vote list by checking whether said extracted tag is the tag of said voter.

16. The electronic voting system of claim 11, wherein: said counter apparatus has a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said each voter apparatus sends said vote data to that one of said plurality of distributed counter apparatuses which is connected to one end of said series connection; and said distributed counter apparatuses comprise decryption parts for sequentially decrypting information containing said encrypted content with said partial secret keys, said vote content being obtained by the decryption processing in said distributed counter apparatus at the last stage of said series connection.

17. The electronic voting system of claim 11, wherein: said

AB
counter apparatus has a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said each voter apparatus sends said vote data to all of said plurality of distributed counter apparatuses; said plurality of distributed counter apparatuses each have a decryption part for decrypting said encrypted vote content with said partial secret key assigned thereto to generate decrypted intermediate data and for sending said decrypted intermediate data to a predetermined one of said distributed counter apparatuses; and said predetermined distributed counter apparatus has a total decryption part for decrypting all of said decrypted intermediate data to obtain said vote content.

18. The electronic voting system of claim 16 or 17, wherein said decryption part performs thresholding decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.

19. A voter apparatus in an electronic voting system which comprises a plurality of said voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a nonanonymous communication channel, and a counter apparatus connected to each of said voter apparatuses through an anonymous communication channel, said voter apparatus comprising:

an encryptor for encrypting a vote content of a voter of said each voter apparatus with a public key of said counter apparatus to generate an encrypted vote content;

a random generator for generating a random number;
a randomizer for randomizing information containing said encrypted vote content with said random number to create a preprocessed text;

AB voter signature generating means for generating a voter signature for said preprocessed text;

means for sending said preprocessed text and said voter signature to said administrator apparatus;

a derandomizer supplied with a blind signature of an administrator for said preprocessed text received from said administrator apparatus and said random number, for excluding the influence of said random number from said administrator blind signature to obtain an administrator signature for said information containing said encrypted vote content;

a signature verification part supplied with said administrator signature for said encrypted vote content and said information containing said encrypted vote content, for verifying the validity of said administrator signature;

means for sending said administrator signature and said information containing said encrypted vote content, as vote data, to said counter apparatus when said administrator signature is found valid; and

a list checking part for making a check to see if vote data of said voter is contained in a vote list received from said counter apparatus.

20. The voter apparatus of claim 19, which further comprises a tag generator for generating a tag that only said voter knows, and a concatenator for concatenating said encrypted vote content with said

tag, and wherein said list checking part extracts said tag from each vote data on said vote list received from said counter apparatus and makes a check to see if said vote data of said voter is contained in said vote list by checking whether said extracted tag is the tag of said voter.

AB
21. A counter apparatus in an electronic voting system which comprises a plurality of voter apparatuses, an administrator apparatus connected to each of said voter apparatuses through a nonanonymous communication channel, and said counter apparatus connected to each of said voter apparatuses through an anonymous communication channel, said counter apparatus comprising:

an administrator signature verification part supplied with information containing vote content encrypted by a public key of a counter, received as vote data from said each voter apparatus, and an administrator signature for information containing said encrypted vote content, for verifying the validity of said administrator signature;

a vote list generator for generating a list of said vote data received from said each voter apparatus when said administrator signature is found valid and for publishing said list to a voter of said each voter apparatus in a manner to be accessible therefrom;

a decryptor for decrypting said information containing said encrypted vote content with a secret key corresponding to said public key to obtain the vote content of said voter; and

counter means for counting the number of votes polled for each candidate on the basis of said decrypted vote content.

22. The counter apparatus of claim 21, which further comprises a

03
series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter, and wherein: said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said vote data sent from said each voter apparatus is received by that one of said plurality of distributed counter apparatuses which is connected to one end of said series connection; said distributed counter apparatuses have partial decryption parts for sequentially decrypting information containing said encrypted content with said partial secret keys, and said vote content is obtained by the decryption process of said partial decryption part in said distributed counter apparatus at the last stage of said series connection.

23. The counting apparatus of claim 21, which further comprises a plurality of distributed counter apparatuses, each placed under the control of a different counter, and wherein: said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said plurality of distributed counter apparatuses each have a partial decryption part for decrypting said encrypted vote content with said partial secret key assigned thereto to generate decrypted intermediate data and for sending said decrypted intermediate data to a predetermined one of said distributed counter apparatuses; and said predetermined distributed counter apparatus has a total decryption part for decrypting all of said decrypted intermediate data to obtain said vote content.

24. The counter apparatus of claim 22 or 23, wherein said partial decryption part performs thresholding decryption processing that

requires a predetermined plural number of said distributed counter apparatuses to work together.

25. A recording medium having recorded thereon a program for executing, by a computer, a procedure of a voter apparatus in an electronic voting system which comprises a plurality of said voter apparatuses, an administrator connected to each of said plurality of voter apparatuses through a nonanonymous communication channel, and a counter apparatus connected to said each vote apparatus through an anonymous communication channel, said procedure comprising the steps of:

- (a) encrypting a vote content of an each voter with a public key of said counter apparatus to generate an encrypted content;
- (b) generating a random number;
- (c) randomizing information containing said encrypted vote content with said random number to generate a preprocessed text;
- (d) generating a signature for said preprocessed text;
- (e) sending said preprocessed text and said signature to said administrator;
- (f) excluding, with said random number, the influence of said random number from a blind signature of an administrator for said preprocessed text received from said administrator apparatus to thereby obtain signature of said administrator for said information containing said encrypted vote content;
- (g) verifying the validity of said information containing said encrypted vote content;
- (h) sending said information containing said encrypted vote content and said administrator signature, as vote data to said counter

apparatus if said information containing said encrypted vote content is found valid; and

(i) making a check to see if vote data of said each voter is contained in a vote list received from said counter apparatus.

a3
26. The recording medium of claim 25, wherein: said procedure comprises the additional steps of generating a tag that only said each voter knows, and concatenating said encrypted vote content with said tag to generate said information containing said encrypted vote content; and said step (i) comprises the additional step of extracting said tag from each vote data on said vote list received from said counter apparatus and making a check to see if said vote data of said each voter is contained in said vote list by checking whether said extracted tag is the tag of said each voter.

27. A recording medium having recorded thereon a program for executing, by a computer, a procedure of a counter apparatus in an electronic voting system which comprises a plurality of voter apparatuses, an administrator connected to each of said plurality of voter apparatuses through a nonanonymous communication channel, and said counter apparatus connected to said each vote apparatus through an anonymous communication channel, said procedure comprising the steps of:

(a) receiving, as vote data, from each of said vote apparatuses information containing a vote content of each voter encrypted with a public key of said counter apparatus and an administrator signature for said information and verifying the validity of said administrator signature;

(b) generating, as a vote list, a list of said vote data received from said each voter apparatus, if said administrator is found valid, and publishing said vote list in the form accessible by said each voter;

(c) decrypting said information containing said encrypted vote content with a secret key corresponding to said public key to obtain the vote content of said each voter; and

(d) counting the number of votes polled for each candidate on the basis of said decrypted vote content.

28. The recording medium of claim 27, wherein: said counter apparatus has a series connection of a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys assigned to said plurality of distributed counter apparatuses, respectively; said step (c) comprises the additional step of receiving said vote data sent from said each voter apparatus by that one of said plurality of distributed counter apparatuses which is connected to one end of said series connection, and sequentially performing partial decryption processes of said information containing said encrypted vote content by said distributed counter apparatuses with said partial secret keys assigned thereto, respectively; and said vote content is obtained by said partial decryption process in said distributed counter apparatus at the last stage of said series connection.

29. The recording medium of claim 27, wherein: said counter apparatus has a plurality of distributed counter apparatuses, each placed under the control of a different counter; said secret key is split into partial secret keys, which are assigned to said plurality of

a³
distributed counter apparatuses, respectively; said step (c) comprises the additional steps of receiving said vote data from all of said voter apparatuses by each of said plurality of distributed counter apparatuses, then encrypting said encrypted vote content with said partial secret key assigned to said each distributed counter apparatus to generate decrypted intermediate data, then sending said decrypted intermediate data to said predetermined distributed counter apparatus, and performing, by said predetermined distributed counter apparatus, total decryption processing of all of said decrypted intermediate data sent thereto to thereby obtain said vote content.

30. The recording medium of claim 28 or 29, wherein said step (e) is a step of performing thresholding partial decryption processing that requires a predetermined plural number of said distributed counter apparatuses to work together.